



Technical Specifications Manual for Online Testing

For Technology Coordinators

2014–2015

Published February 12, 2014

Prepared by the American Institutes for Research®



Descriptions of the operation of the Test Information Distribution Engine, Test Delivery System, and related systems are property of the American Institutes for Research (AIR) and are used with the permission of AIR.

Table of Contents

Introduction to the Technical Specifications Manual.....	1
Manual Content	1
Other Resources.....	2
Section I. Network and Internet Requirements	3
General Requirements.....	3
Common Network Performance Bottlenecks.....	4
Bandwidth	4
Determining Bandwidth Requirements	5
Total Number of Students Simultaneously Testing.....	6
Size of the Test Content.....	6
Secure Browser Installation.....	6
Network Configuration	6
Protocols.....	6
Domain Name Resolution.....	7
Content Filter, Firewalls, and Proxy Servers	7
Quality of Service (QoS)/Traffic Shaping	7
Certificate Revocation List.....	7
Symantec Recommendations	7
Wireless Networking and Wireless Access Points	8
Network Diagnostic Tools	9
AIR's Network/Bandwidth Diagnostic Tool	10
Microsoft Windows Specific Tools	10
Mac OS X Specific Tools.....	10
Multi-Platform Tools.....	11
Section II. General Hardware Requirements	12
Monitors and Screen Display Requirements	12
Screen Dimensions	12
Screen Resolution	13
Keyboards.....	13
Headphones	14
Printers.....	14
Section III. General Software Requirements	16
Requirements for All Systems	16

Enabling Pop-Up Windows.....	16
Requirements for Flash	17
Windows Requirements.....	18
Disabling Fast User Switching.....	18
Disabling Fast User Switching in Windows XP.....	18
Disabling Fast User Switching in Windows Vista and Windows 7	19
Disabling Fast User Switching in Windows 8.0 and 8.1.....	20
Enabling Web Fonts in Internet Explorer 10 and 11	22
Installing Windows Media Pack for Windows 8.1 N and KN	23
Mac OS X Requirements.....	24
Disabling Spaces	24
Function Keys and Application Launches	25
Linux Requirements—Installing Verdana TrueType Font	26
Mobile Requirements.....	27
Enabling Guided Access on iOS	27
Configuring Using Autonomous Single App Mode	27
Overview of Autonomous Single App Mode and the Secure Testing Environment	28
Step 1: Create a Mobile Device Management Profile.....	28
Step 2: Create a Supervisory Profile.....	29
Step 3: Place iPads in Autonomous Single App Mode	31
Enabling the Secure Browser Keyboard on Android.....	34
Enabling Kiosk Mode and Wiping Chrome OS.....	36
Section IV. Text-to-Speech Requirements.....	37
Overview of Text-to-Speech	37
Using Text-to-Speech.....	37
How the Secure Browsers Work With Voice Packs	37
Desktop Secure Browsers.....	37
Mobile Secure Browsers	38
About NeoSpeech™ Voice Packs for Windows	38
Windows Text-to-Speech Settings	39
Mac OS X Text-to-Speech Settings.....	40
Linux Text-to-Speech Settings	41
Voice Packs Recognized by Desktop Secure Browsers	42
Windows	42
Mac OS X	43

Linux	44
Appendix A. Systems and URLs Provided by AIR	45
Non-Testing Sites	45
Testing Sites	45
TA and Student Testing Sites.....	45
Online Dictionary and Thesaurus	45
Appendix B. Technology Coordinator Checklist	46
Appendix C. User Support	48

List of Tables

Table 1. Key Symbols and Elements	1
Table 2. Average Bandwidth Used by Secure Browser for Testing.....	5
Table 3. Ports for Test Delivery System	7
Table 4. Wireless Access Points.....	9
Table 5. Flash Requirements.....	17
Table 6. Commands for Installing Voice Packs on Linux Distributions.....	41
Table 7. Voice Packs Recognized by Secure Browsers—Windows.....	42
Table 8. Voice Packs Recognized by Secure Browsers—Mac OS X.....	43
Table 9. Voice Packs Recognized by Secure Browsers—Linux.....	44

Introduction to the Technical Specifications Manual





This manual provides information about network and Internet requirements, general hardware and software requirements, and text-to-speech information—all of which are required for running various testing applications provided by American Institutes for Research (AIR).

Manual Content

Below is a brief description of each section in this manual, as well as common symbols and elements used throughout the document.

- [Section I, Network and Internet Requirements](#), provides information about bandwidth, networking, and available diagnostic tools.
- [Section II, General Hardware Requirements](#), outlines requirements for monitors and screen displays, keyboards, headphones, and printers.
- [Section III, General Software Requirements](#), outlines required configurations for desktop operating systems (Windows, Mac, and Linux).
- [Section IV, Text-to-Speech Requirements](#), contains information for ensuring text-to-speech settings are enabled on desktop operating systems. Information about voice packs for Windows is also included.
- The appendices contain URLs for systems provided by the American Institutes for Research, a checklist for system administrators and technology coordinators, and a sample scheduling worksheet.

Table 1. Key Symbols and Elements

Element	Description
	Warning: This symbol accompanies important information regarding actions that may cause fatal errors.
	Alert: This symbol accompanies important information regarding a task that may cause minor errors.
	Note: This symbol accompanies additional information that may be of interest.
text	Bold text indicates a link or button that is clickable.
	Tip: This symbol accompanies suggestions that may be useful.

Other Resources

- For information about supported operating systems, refer to the *System Requirements* document.
- For information about installing secure browsers, refer to the *Secure Browser Installation Manual*.
- For information about Braille hardware and software requirements, as well as basic test administration processes, refer to the *Braille Requirements* document.

The above resources as well as test administration manuals and user guides for other systems are available on the MEA Mathematics and English Language Arts/Literacy portal (<https://me.portal.airast.org>).

Section I. Network and Internet Requirements

The information in this section provides an overview of network and Internet configuration requirements and available diagnostic tools.

General Requirements

A stable, high-speed (wired or wireless) Internet connection is required for online testing. The response time for each assessment depends on the reliability and speed of your school's Internet network.

If your Internet connection is not working or stops working, students will need to complete their tests at a later time or on another day. Any answers they have already submitted will be saved, and students will resume their tests where they left off. (Students will return to the first unanswered item in the test.)

For the online testing applications to work properly, you may need to verify your network settings. If you are not sure whether your network is properly configured or you have questions, contact your network administrator or technology specialist to find the right contact person in your area. You may also contact the MEA Mathematics and English Language Arts/Literacy Help Desk.

Network configuration settings should include the following:

- Content filters, firewalls, and proxy servers should be configured to allow traffic on the protocols and to the servers listed below.
- Session timeouts on proxy servers and other devices should be set to values greater than the average scheduled testing time. If testing sessions are scheduled for 60 minutes, consider session timeouts of 65–70 minutes. This will help limit network interruptions during testing.
- Data cannot be cached.
- If your client network uses any devices that perform traffic shaping, packet prioritization, or Quality of Service, the URLs for the systems provided by AIR should be given a high priority to guarantee the highest level of performance.

For information about URLs that should be open or whitelisted, refer to [Systems and URLs Provided by AIR](#).

Common Network Performance Bottlenecks

All network communications are accomplished using the IP protocol suite. The local area network (LAN) must be able to route IP traffic to and from the Internet.

The Test Delivery System is delivered directly through the Internet. Students must access their tests using the appropriate secure browser. For testing to take place, all workstations where tests will be administered must have reliable Internet connectivity.

In general, the performance of the Test Delivery System will depend on a number of factors, including bandwidth, total number of students simultaneously testing, size of test content, secure browser installation, proxy server (if used), and the wireless networking solution (if used).

Bandwidth

Bandwidth is the measure of the capacity of a network. Utilized bandwidth measures the amount of data traveling across the network at a given point in time. Bandwidth performance can be affected on either the internal network (LAN) traffic or the Internet traffic from the router. Regardless of hardware or network topology, the LAN should be analyzed to determine the potential for traffic bottlenecks.

[Table 2](#) displays the estimated average bandwidth used by the secure browser for testing. (Note that there is a one-time exception to these averages; during initial secure browser startup, the load can be greater, leading to a longer load time.) All numbers provided are based on rigorous testing using Wireshark.

Table 2. Average Bandwidth Used by Secure Browser for Testing

Number of Students Testing Concurrently in School/Building	Average Estimated Bandwidth Consumed During Subsequent Startup of Secure Browser ^a	Average Estimated Bandwidth Consumed During Testing ^b
1	8 Kbps	5–15 Kbps
50	400 Kbps	250–750 Kbps (0.25–0.75 Mbps)
100	800 Kbps	500–1500 Kbps (0.5–1.5 Mbps)

^a Bandwidth consumed when opening the secure browser and accessing an assessment for the first time is significantly higher than when opening the secure browser and accessing an assessment subsequently. The reason for this is that the initial launch of the secure browser downloads non-secure cacheable content (not test content) that can be immediately accessed upon opening the secure browser at a later time.

^b Bandwidth will vary during a student's testing experience, as some pages contain low-bandwidth content, such as multiple-choice items, and other pages contain higher-bandwidth content, such as animations, audio clips, or American Sign Language videos. Consequently, the estimated average values in this column are based on computing averages from multiple assessments and subjects.

Determining Bandwidth Requirements

Schools need to factor the bandwidth requirements of each assessment along with all other non-testing-related Internet traffic in order to determine how many concurrent test sessions their Internet connections can support.

- Some assessments include animations and interactive item types. These may increase the bandwidth required, but the bandwidth should not exceed the peak usage experienced when the test initially loads. **We encourage you to run the diagnostics on your network to determine how many students you can reasonably test at one time.** For information about running diagnostics on your network, refer to the [Network Diagnostic Tools](#) section.
- For wired networks, internal bandwidth is typically not a problem, because new switches generally operate at speeds of between 100 Mbps and 1000 Mbps. However, LAN performance can be hindered in cases where hubs are used instead of switches. A hub device will allow broadcast signals from various network devices to propagate across the network, potentially saturating the network and causing traffic competition and/or collisions of data.

- For Internet networks, the most common bottleneck is the ISP's router connection, which typically operates at speeds of between 1.5 Mbps and 100 Mbps. Network administrators should spend time prior to test administration determining whether their Internet infrastructure has the capacity to accommodate current and future growth.

**Analyzing Infrastructure**

Determining whether infrastructure is capable of current and future growth involves a number of steps, including but not limited to (1) the analysis of the current number of users; (2) current day-to-day Internet bandwidth statistics; and (3) the desired response time for applications.

Total Number of Students Simultaneously Testing

As the number of students testing at one time increases, competition for network bandwidth increases. Network bandwidth resembles highway traffic; as the number of cars traveling on a given road increases, the speed of traffic flow decreases.

Size of the Test Content

The size of the test is determined by two factors: (1) the number of items on the test and (2) the average size of each item. The more items a test contains and the larger the average size of a test item, the higher the bandwidth requirement for a given test. For example, ELA tests typically deliver all items associated with a passage at one time, and this may slightly impact the bandwidth for these tests.

Secure Browser Installation

The recommended installation of the secure browser is local installation on each individual testing workstation. It may be possible to install the secure browser on a network or shared drive and then have the testing workstations run the secure browser from that drive, but there may be some performance impacts under this configuration. There will be competition for network bandwidth, and the network or shared disk drive will also be subject to some resource competition as there will be multiple clients reading from the network drive, thus slowing the overall processing speed.

Network Configuration**Protocols**

All communication with the Test Delivery System takes place over the Internet port/protocol combinations shown in Table 3. Please ensure that the following ports are open for these systems.

Table 3. Ports for Test Delivery System

Port/Protocol	Purpose
80/tcp	HTTP (initial connection only)
443/tcp	HTTPS (secure connection)

Domain Name Resolution

All system URLs must be resolvable by all client hosts attempting to connect to the Test Delivery System. This means that the client workstations should be able to convert the friendly names (URLs) to their corresponding IP address by requesting the information from the DNS server.

For a list of URLs, refer to [Appendix A, Systems and URLs Provided by AIR](#).

Content Filter, Firewalls, and Proxy Servers

Content filters, firewalls, and proxy servers should be configured to allow traffic on the protocols listed above to the applications' servers.

In addition, session timeouts on proxy servers and other devices should be set to values greater than the average duration it takes a student to participate in a test session or complete a given test. For example, if your school determines that students will test in 60-minute sessions, then consider setting the session timeout to 65 or 70 minutes.

System administrators will need to make sure that information is not blocked in their content filters and that data are not cached. The URLs listed in Appendix A should be open for these systems.

Quality of Service (QoS)/Traffic Shaping

If the client network utilizes any devices that perform traffic shaping, packet prioritization, or Quality of Service, the URLs should be given a high level of priority in order to guarantee the highest level of performance.

Certificate Revocation List

Schools should open their firewalls to allow the secure browser to check the certificate authenticity at Symantec Certificate Revocation List (CRL) at <http://crl.verisign.com/>.

Symantec Recommendations

Note: The following information was provided by [Symantec](#).

It is strongly recommended that any firewall policies and/or access control devices use URLs and not IP addresses. Symantec can change these IP addresses at any time without notification.

If possible, white list the following entries on your firewall policies and/or access control devices to ensure seamless access to our Online Certificate Status Protocol (OCSP) services:

- *.thawte.com
- *.geotrust.com
- *.ws.symantec.com

Note: If white listing wildcard entries is not permitted, you can white list the following specific fully qualified domain names (FQDNs):

- oscp.ws.symantec.com
- oscp.geotrust.com
- oscp.thawte.com

If your firewall is configured to allow only a certain set of IP addresses to be accessed from your network, you will need to take the following actions:

- [Get the full list of IP addresses for the new sites](#). Complete a short form and then you will gain access to the site list.
- Install or add the IP addresses to your existing list. Do not replace the old IP addresses and your existing rules for Symantec OCSP IP addresses should not be deleted.

Wireless Networking and Wireless Access Points

Over the past several years, there have been several revisions to wireless networking technology.

- 802.11ac has a theoretical throughput of up to 1 gigabit per second.
- 802.11n has a throughput of up to 300 Mbps.
- 802.11g has a theoretical throughput of up to 54 Mbps.
- 802.11b has a theoretical throughput of 11 Mbps.



Wireless Security

Due to the sensitivity of test-related data, it is highly recommended that wireless traffic use WPA2/AES data encryption. Because encryption/decryption is part of the data exchange process, there may be a slight decrease in the overall speed of the network. A properly configured wireless network should provide adequate bandwidth for the testing applications.

AIR recommends that schools maintain a ratio of wireless systems to wireless access points (WAPs) of no more than 20 to 1. Typically, the test performance begins to deteriorate after that threshold has been reached. In some instances, older WAPs may also see performance degradation when more than 15 devices are concurrently connected.

Recommendations on the optimal number of student workstations per wireless connection:

The optimal (or maximum) number of student workstations (computers and tablets) supported by a single wireless connection depends on the type of networking standard being used for the connection. The two most common networking standards are 802.11g (54 Mbps) and the newer and faster standard 802.11n (300 Mbps). Both the access point, which emits the wireless signal, and the computer's wireless card, which receives the signal, will use one of these two standards. The recommendations in [Table 4](#) are based on the standard in use. Refer to your WAP documentation for specific recommendations and guidelines.

Table 4. Wireless Access Points

Interface	802.11g Access Point	802.11n Access Point
802.11g Wireless Cards	20 workstations or devices	40 workstations or devices
802.11n Wireless Cards	20 workstations or devices	40 workstations or devices
Mix of 802.11g and 802.11n Wireless Cards	20 workstations or devices	40–50 workstations or devices (depending on the ratio of wireless cards used)

Network Diagnostic Tools

A performance analysis of the LAN/Internet infrastructure is recommended in order to identify any bottlenecks that may impact test performance. Identifying the diagnostic tool most appropriate for a network depends on the testing operating system, the network administrator's knowledge base, and the desired level of network analysis. A number of network diagnostic tools are available, as described in the following sections.

AIR's Network/Bandwidth Diagnostic Tool

AIR provides a diagnostic tool that can be directly accessed from the student test login page.

1. On the test login page, click the **Run Diagnostics** link. The Diagnostic Screen page will display.
2. In the *Network Diagnostics* section, select a test.
3. Select the approximate number of students who may take that test *at one time*.
4. Click the **Run Network Diagnostics Tests** button.

The results will display your current upload and download speed as well as a general idea of whether you can reliably test the given number of students (the number entered in step 3). You may want to run this test several times throughout the day to verify that your upload and download speeds remain relatively consistent.

Microsoft Windows Specific Tools

PRTG Traffic Grapher

PRTG (www.paessler.com/prtg) monitors bandwidth usage and other network parameters via Simple Network Management Protocol (SNMP). It also contains a built-in packet sniffer. A freeware version is available.

NTttcp

NTttcp (www.microsoft.com/whdc/device/network/TCP_tool.msp) is a multithreaded, asynchronous application that sends and receives data between two or more endpoints and reports the network performance for the duration of the transfer.

Pathping

Pathping is a network utility included in the Windows operating system. It combines the functionality of Ping with that of Traceroute (Windows filename: `tracert`) by providing details of the path between two hosts and Ping-like statistics for each node in the path based on samples taken over a time period.

Mac OS X Specific Tools

Network Utility.app

This tool is built into Mac OS X software.

Multi-Platform Tools

Wireshark

Wireshark (www.wireshark.org) is a network protocol analyzer. It has a large feature set and runs on most computing platforms including Windows, OS X, Linux, and UNIX.

TCPDump

TCPdump (<http://sourceforge.net/projects/tcpdump>) is a common packet sniffer that runs under the command line and is compatible with most major operating systems (UNIX, Linux, Mac OS X). It allows the user to intercept and display data packets being transmitted or received over a network.

A Windows port WinDump is also available (www.winpcap.org/windump/).

Ping, NSLookup, Netstat, Traceroute

This is a set of standard UNIX network utilities. Versions of these utilities are included in all major operating systems (UNIX, Linux, Windows, and Mac OS X).

Iperf

Iperf (<http://sourceforge.net/projects/iperf/>) measures maximum TCP bandwidth, allowing the tuning of various parameters and User Datagram Protocol (UDP) characteristics. Iperf reports bandwidth, delay jitter, and datagram loss.

Section II. General Hardware Requirements

The following information is general. Because of the myriad ways school computers can be set up, we encourage you to verify that all related hardware is configured correctly.



About Braille Requirements

This manual does not contain information about required hardware for students taking online assessments with Braille support. For information about Braille hardware and software requirements, refer to the *Braille Requirements* document, which is available on the MEA portal.

Monitors and Screen Display Requirements

All supported computers, laptops, netbooks, and tablets must meet the following requirements.

Screen Dimensions

Screen dimensions must be at least 10" (note that iPads with a 9.5" display are included). This means the following devices are not supported:

- Apple iPad Mini
- Google Nexus 7 and similar-sized Android tablets
- Netbooks with screen dimensions smaller than 10"

Screen Resolution

All devices must meet the following minimum resolution. Larger resolutions can be applied as appropriate for the monitor or screen being used.

- Desktops, laptops, and tablets: 1024 × 768
- Netbooks: 1024 × 600

Depending on the screen size, students may need to use vertical or horizontal scroll bars to view all test-related information. Students may also use the Zoom tool in the online test to enlarge the content on the screen.



Alert: Common Issues with Brightness and Contrast

Some test items include images that are shaded. Because monitors and screens vary widely, we cannot guarantee that the “default” settings on monitors are optimal. Monitor settings may need to be adjusted if a student says test items with shaded images (e.g., pie charts) are very light or cannot be seen.



Alert: Computers with Dual Monitors Poses Security Risk

Students should not take online tests on computers that are connected to more than one monitor. Systems that use a dual monitor setup typically display an application on one monitor while another application is accessible on the other monitor.

Keyboards

The use of external keyboards is strongly recommended for tablets that will be used for testing.

Students may use mechanical, manual, and Bluetooth-based keyboards. While wireless keyboards are permissible, districts should be aware that high-density deployments of wireless keyboards and mice might interfere with each other or with the wireless network. Some external keyboards have additional “shortcut” buttons that can create security issues. These buttons may allow students to open another application or the tablet’s default on-screen keyboard. AIR strongly cautions against using keyboards that have these shortcut buttons.

For Android tablet users:

The Android mobile secure browser requires the secure browser keyboard to be used because the default tablet keyboard includes a row for predictive text. Therefore, any external keyboard that has a shortcut button to open the tablet's default keyboard is not permitted, as this default keyboard will override the mobile secure browser keyboard.

AIR has determined that the following external keyboard contains a shortcut button that opens the default keyboard and should NOT be used with Android tablets:

- EZOWare Slim Full Size Keyboard

Headphones

Students will need headphones to listen to audio in the assessments.

- Some assessments contain several items that have recorded audio.
- Students who are using text-to-speech can listen to stimuli or test items being read aloud.
- Students who use Braille can use the Job Access with Speech (JAWS®) screen reading software.

Test Coordinators should determine how many students will need headphones prior to testing to ensure that there is an adequate supply on hand.



Note: USB headphones are recommended, as they are typically plug-and-play devices.

Text-to-speech requires the use of the secure browser. Students who require text-to-speech for the practice tests should use the secure browser.

Printers

Test Administrators can print out test session information and can approve student requests to print stimuli or test items (for students with the print-on-request accommodation). In order to preserve test security, Test Administrators must follow the test security protocols for printed test materials.

We strongly suggest that Test Administrators be connected to a single local or network printer in the testing room. Only the Test Administrator's computer should have access to this printer.

**Special Note Regarding Wireless Printing**

Apple iOS devices have native printing support (AIR Print), which connects to printers on a wireless network. Devices that have an Android or Chrome operating system or Chrome browser allow people to use the Google Cloud Print option.

If users need to print, it is recommended that they use a computer or device with a direct connection to a printer.

**About Braille Devices**

For information about Braille devices and related software, refer to the *Braille Requirements* document, which is available on the MEA portal.

Section III. General Software Requirements

In addition to installing the secure browser, you may need to adjust operating system settings or install additional software on students' machines that are used for testing.



About Braille Requirements

This manual does not contain information about required software for students taking online assessments with Braille support. For information about Braille hardware and software requirements, refer to the *Braille Requirements* document, which is available on the MEA portal.

Requirements for All Systems

Enabling Pop-Up Windows

All systems provided by AIR except for the secure browser require pop-up windows to be enabled. These systems use pop-up windows to provide warning or error messages to users.

Navigate to the appropriate menu option to globally disable pop-up blockers.

To globally enable pop-up windows:

- **Firefox:** Tools > Options > Content > clear **Block pop-up windows**.
- **Google Chrome:** Menu > Settings > Show advanced settings (at the bottom of the screen) > Privacy > Content Settings > Pop-ups > mark **Allow all sites to show pop-ups**.
- **Chrome browser on Android tablets:** Menu > Settings > Advanced > Content Settings > Block pop-ups > clear checkbox.
- **Internet Explorer:** Tools > Pop-up Blocker > **Turn Off Pop-up Blocker**.
- **Safari:** Application Menu (Safari) > clear **Block Pop-Up Windows**.
- **iOS Safari:** Settings > Safari > Block Pop-ups (toggle to "off" mode).

If you want to only allow certain sites to have pop-up windows, you can add exceptions and whitelist AIR's systems. For URLs and information about whitelisting, refer to [Appendix A, Systems and URLs Provided by AIR](#).

To add exceptions to the pop-up blocker:

- **Firefox:** Tools > Options > Content > click **Exceptions**. Enter the URL or whitelist protocol for each system.
- **Google Chrome:** Menu > Settings > Show advanced settings (at the bottom of the screen) > Privacy > Content Settings > Pop-ups > click **Manage Exceptions**. Enter the URL or whitelist protocol for each system and select **Allow**. This option is not available for the Chrome browser on Android tablets.
- **Internet Explorer:** Tools > Pop-up Blocker > Pop-up Blocker Settings. Enter the URL or whitelist protocol for each system and click **Add**. Configure other settings as desired.
- **Safari and iOS Safari:** N/A

Requirements for Flash

Some test items require Flash (not applicable for tablet secure testing application). [Table 5](#) lists the requirements for installing Flash on the testing computers.

Table 5. Flash Requirements

Browser	Flash Requirement
Secure browser 7.0 and later	Flash included in the secure browser, no need for additional installation.
Secure browser 6.5	Flash bundled in the secure browser installation pack.
Secure browser 5.6	Flash bundled in the secure browser installation pack.
Commercial browser* with HTML5	Flash included in the browser, no need for additional installation.
Commercial browser* before HTML5	Install Flash for your operating system, or install the Flash plug-in for the browser.

*Commercial browsers—the versions of Internet Explorer, Chrome, Safari, and mobile browsers listed in the *Online System Requirements*.

Windows Requirements

This section contains information specific to Windows users.

Disabling Fast User Switching

Microsoft Windows (XP, Vista, 7, 8.0, and 8.1) allows computers to be configured to allow multiple users to log in to a computer without requiring one user to log out before another logs in. This feature is called “Fast User Switching” and presents a test security risk if it is enabled.

If a student can access multiple user accounts from a single computer, you are required to disable the Fast User Switching function. The following sections describe how to disable Fast User Switching in supported versions of Windows.

Disabling Fast User Switching in Windows XP

1. Click Start, click Control Panel, then click User Accounts.
2. Click Change the Way Users Log On or Off.
 - a. Ensure the **Use the Welcome Screen** option is checked.
 - b. Ensure the **Use Fast User Switching** option is *not* checked.
3. Click Apply Options.

*Fast User Switching is not an option if joined to a domain.

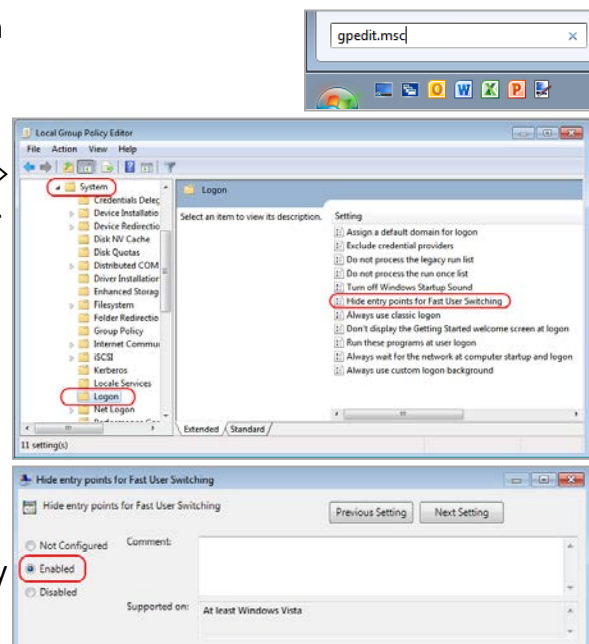


Disabling Fast User Switching in Windows Vista and Windows 7

Option A: Access the Group Policy Editor

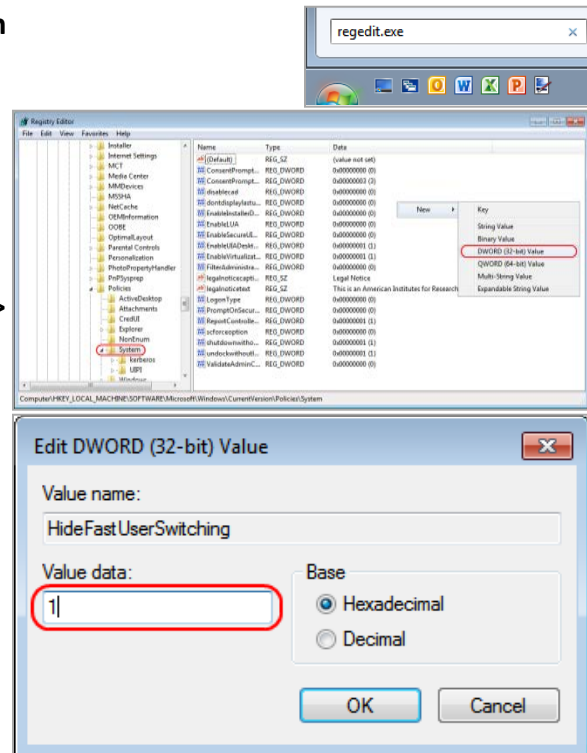
1. Click **Start**, type `gpedit.msc` in the **Start Search** dialog box, and press **Enter**.
2. Navigate to the following location: Local Computer Policy > Computer Configuration > Administrative Templates > System > Logon.
3. Double-click **Hide entry points for Fast User Switching**. A properties dialog box appears.
4. Mark **Enabled**, and click **OK**.
5. Close the Local Group Policy Editor window.

Note: Because the Group Policy Editor does not exist in certain editions of Windows Vista, you may need to configure these settings via the registry. See below for registry instructions.



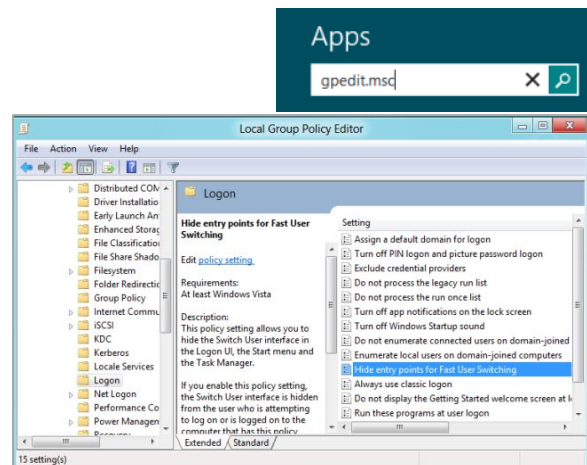
Option B: Access the Registry

1. Click **Start**, type **regedit.exe** in the **Start Search** dialog box, and press **Enter**.
2. Navigate to the following location:
HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Policies > System.
3. Right-click the **System** folder, and select **New > DWORD (32-bit) value**.
4. Type **HideFastUserSwitching** and press Enter.
5. Double-click the **HideFastUserSwitching** key.
6. In the *Value data* field, type **1**, and then click **OK**.
7. Close the Registry Editor window.

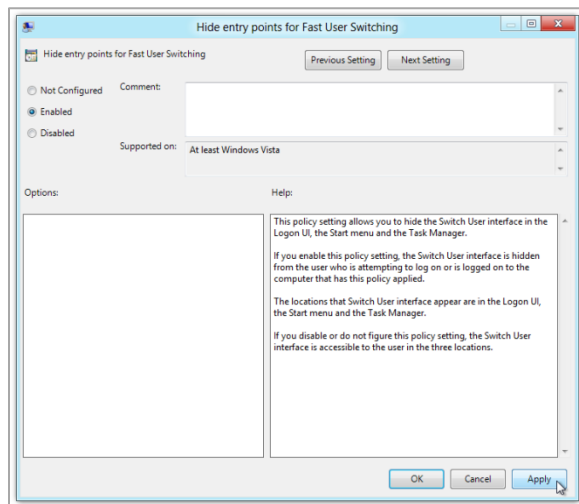


Disabling Fast User Switching in Windows 8.0 and 8.1

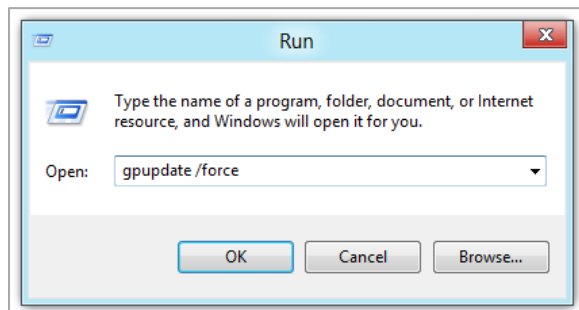
1. Navigate to the Search option. (From the home screen, mouse to the lower right corner and then click the Search icon.)
2. In the search box, type **gpedit.msc**. Double-click the **gpedit** icon in the Apps pane. The Local Group Policy Editor window will open.
3. Navigate to the following location: Computer Configuration > Administrative Templates > System > Logon.
4. In the Setting pane, double-click "Hide entry points for Fast User Switching."



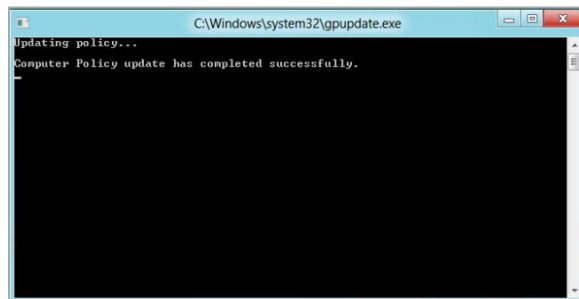
5. Select “Enabled” and then click **OK**.



6. Navigate to the Search option (from the home screen, mouse to the lower right corner and then click the Search icon).
7. In the search box, type **run**. The Run dialogue box will open.
8. Enter the command **gpupdate /force** into the text box and then click **OK**. *(Note the space before the backslash).*



9. The Windows system command box will open. When you see the message “Computer Policy update has completed successfully,” then Fast User Switching has been successfully disabled.

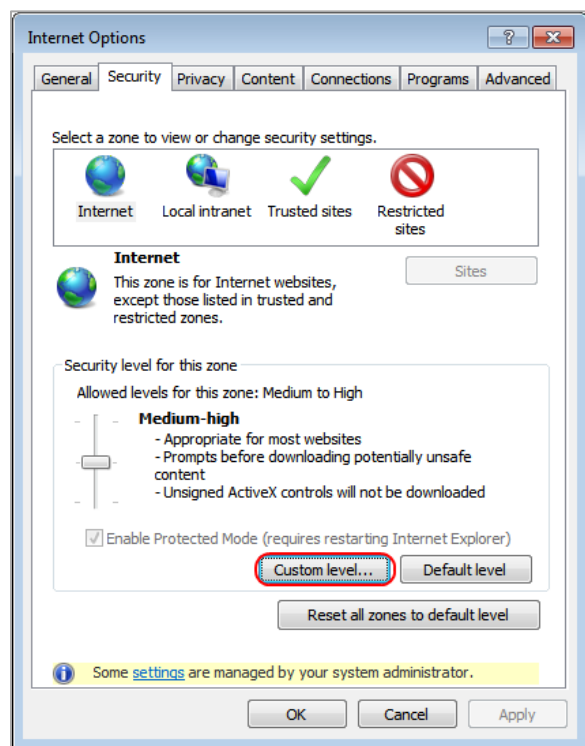


Enabling Web Fonts in Internet Explorer 10 and 11

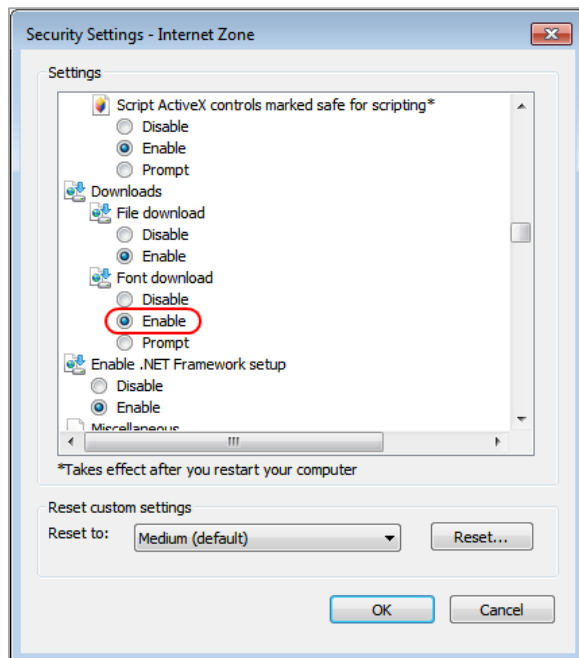
If students use Internet Explorer 10 or 11 to access the practice tests, web fonts may need to be enabled in order for some item types to display properly.

Enabling Web Fonts in Internet Explorer:

1. Open the **Tools** menu in Internet Explorer and click **Internet Options**. The Internet Options window will open.
2. Click the **Security** tab.
3. Click the **Custom Level** button. The Security Settings window will open.



4. Scroll to “Font Download” in the Settings list and click the **Enable** radio button.
5. Click **OK**. The Security Settings Window will close.
6. Click **OK**. The Internet Options window will close.



Installing Windows Media Pack for Windows 8.1 N and KN

Some versions of Windows 8.1 are not shipped with media software installed. As a result, you may need to install software in order for students to listen to audio as well as watch videos.

Microsoft provides additional information as well as a download package for computers with the following Windows 8.1 versions:

- Windows 8.1 N
- Windows 8.1 N/K with Bing
- Windows 8.1 Enterprise N
- Windows 8.1 Pro N
- Windows 8.1 Pro N/K for EDU

AIR encourages downloading this software and ensuring it works with sample websites and video and audio files prior to installing the Windows secure browser. Installation instructions are provided on Microsoft’s download page.

Microsoft Resources:

- [About the Media Feature Pack for Windows 8.1 N and Windows 8.1 KN Editions: April 2014](http://support.microsoft.com/kb/2929699/en-us)
(http://support.microsoft.com/kb/2929699/en-us)
- [Download Media Feature Pack for N and KN Versions of Windows 8.1](http://www.microsoft.com/en-us/download/details.aspx?id=42503)
(http://www.microsoft.com/en-us/download/details.aspx?id=42503)

Mac OS X Requirements

This section contains information specific to Mac OS X users. These settings can be configured before or after installing the secure browser.

Disabling Spaces

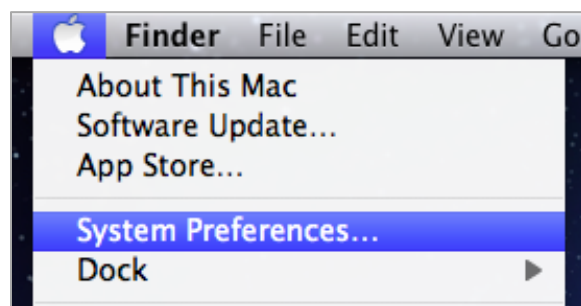
For security purposes, Spaces must be disabled on computers that students will use for online testing. If Spaces is not disabled, students will be unable to test.

Spaces must be disabled on computers running Mac 10.7, 10.8, 10.9, and 10.10.

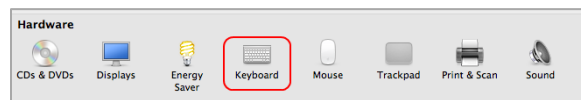
Note: The instructions in this section are for disabling Spaces on individual Mac computers.

To disable Spaces in Mission Control:

1. Navigate to Apple → System Preferences



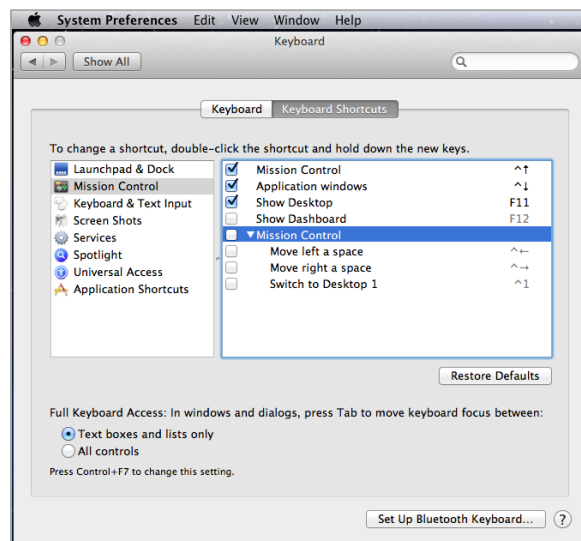
2. In System Preferences, click the **Keyboard** icon. The Keyboard window will be displayed.



3. Click the **Keyboard Shortcuts** or **Shortcuts** tab. The Keyboard Shortcuts options will be displayed.



4. In the left panel, click “Mission Control.”
The right panel will show all Mission Control options.
5. In the right panel, make sure the boxes for the following are NOT checked:
 - a. Move left a space
 - b. Move right a space
 - c. Switch to Desktop 1 (this may already be unchecked)



6. To re-enable Spaces, follow steps 1–4 again, and check the boxes for spaces.

Function Keys and Application Launches

When students use the secure browser for testing, the Test Delivery System conducts regular checks to ensure that other applications are not open. These checks help maintain the integrity of the secure test environment.

Some Mac computers are configured to launch iTunes and other applications by pressing the function keys (e.g., F8) on the keyboard. This section contains information on how to prevent the function keys from directly launching applications, including iTunes. This action will help prevent students from accidentally pressing a function key instead of a key in the number row.

These instructions are based on Mac 10.9 and should be similar for other supported Macs.

To modify the function keys:

1. Open **System Preferences**.
2. In the Hardware row, click **Keyboard**. The Keyboard window opens.

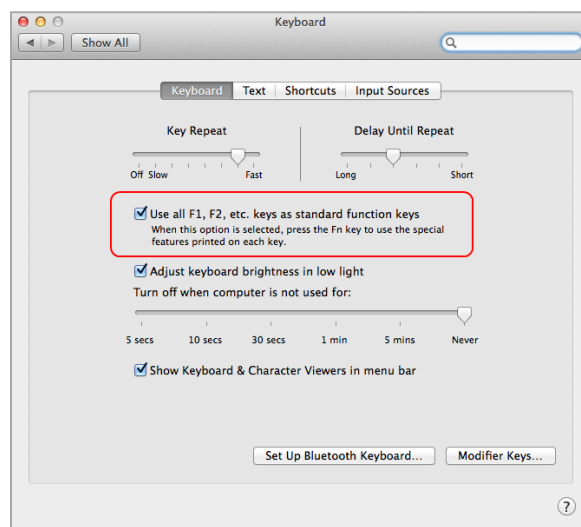


3. In the Keyboard window, mark the **Use all F1, F2, etc. keys as standard function keys**.

You should no longer be able to launch applications with just the function keys.

If you need to launch iTunes or another application, press the Fn key and then press the desired function key. This combination will launch the application.

Important: If a student is testing with the secure browser and presses the Fn key and a function key, this action will open the linked application and result in the test being paused.



Linux Requirements—Installing Verdana TrueType Font

This section contains information specific to Linux users. (Information about installing and enabling text-to-speech settings appears in [Linux Text-to-Speech Settings](#).)

Some assessments have content that uses the Verdana TrueType font. You must ensure that Verdana is appropriately installed on all Linux machines that will be used for testing.

- Fedora, Red Hat, and openSUSE—Follow the steps in the “How to Install” section of the following website: <http://corefonts.sourceforge.net/>. You will need to build an rpm package of the fonts prior to installing them.
- Ubuntu—In a terminal window, enter the following command to install the msttcorefonts package:

```
sudo apt-get install msttcorefonts
```

Mobile Requirements

This section provides a brief overview of the requirements for student testing on tablets and Chromebooks.

Enabling Guided Access on iOS

Guided Access restricts the iOS to a single application and prevents taking screenshots. This ensures a secure test environment. (You may want to use Single App mode, which is easier to enable and activate than Guided Access; for more details about this configuration, see [Configuring Using Autonomous Single App Mode.](#))

The procedure in this section only *enables* Guided Access; to *activate* guided access before a test, see the *Test Administrator User Guide*.

To enable Guided Access:

1. Tap **Settings**.



2. Navigate to General > Accessibility > Learning, and turn on **Guided Access**.
3. Set the passcode for Guided Access. (Test Administrators use this passcode to deactivate Guided Access after a test.)
 - a. Tap **Set Passcode**.
 - b. Enter a passcode.
 - c. Confirm the passcode.
4. Save the passcode in a safe place. There is no ability to retrieve a forgotten passcode.



Configuring Using Autonomous Single App Mode

If you have iOS tablets running version 7.1 or higher, and if you have a Mac running version 10.10 or higher, then you can use Autonomous Single App Mode (ASAM) to quickly create a secure testing environment on all iPads used for testing. (Tablets running a version earlier than

7.1 require Guided Access; for details about this configuration, see [Enabling Guided Access on iOS.](#)) Compared to Guided Access, ASAM requires less time to prepare for test sessions; there is no need to activate Guided Access on each iPad before each test session.

Overview of Autonomous Single App Mode and the Secure Testing Environment

To manage multiple iPads using ASAM, you need to do the following:

[Step 1: Create a Mobile Device Management Profile](#)

[Step 2: Create a Supervisory Profile](#)

[Step 3: Place iPads in Autonomous Single App Mode](#)

After completing these three steps, each time a student starts a test, the iPad enters ASAM and the test environment is secure.

Step 1: Create a Mobile Device Management Profile

The first step in provisioning iPads with ASAM is to create a mobile device management (MDM) profile. No special settings are required in the profile—all default settings are compatible. Deploy the profile to a host that the iPads can access.

Creating an MDM profile is beyond the scope of this specification manual. The following references provide introductory information:

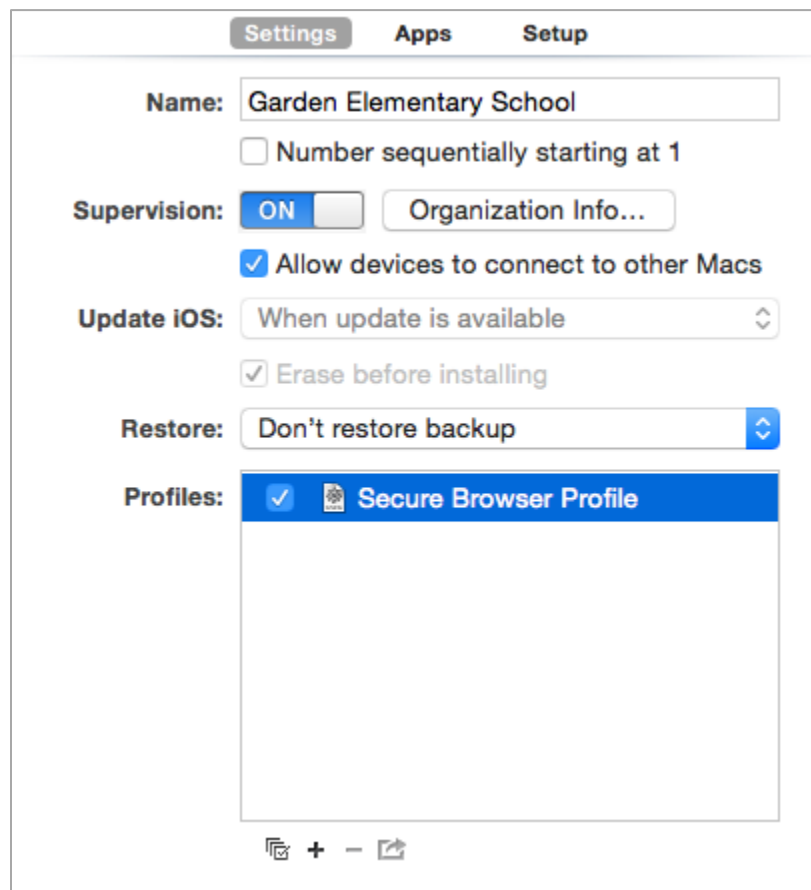
- *IT in the Classroom*, available at <https://www.apple.com/education/it/mdm/>.
- *Apple Configurator Help*, available at <https://help.apple.com/configurator/mac/1.0/#>.
- *Pro tip: Use OS X Server Profile Manager for MDM*, available at <http://www.techrepublic.com/article/pro-tip-use-os-x-server-profile-manager-for-mdm/>.

Step 2: Create a Supervisory Profile

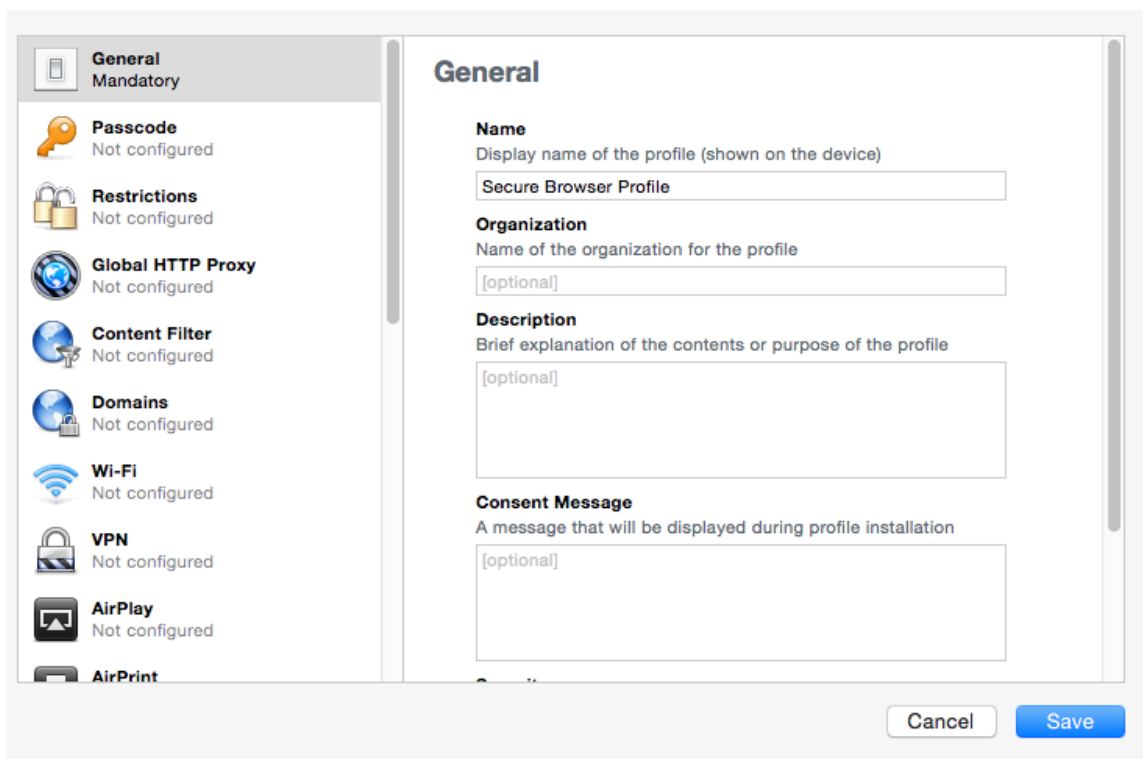
To create a supervisory profile:

1. On a Mac 10.10, download and install Apple Configurator from the Mac App Store. When the installation completes, open Apple Configurator.
2. Click **Prepare**, then **Settings**. The Settings window appears, as shown in Figure 1.

Figure 1. Settings Window in Apple Configurator



- Click + below the Profiles list and select **Create New Profile....** A configuration window appears.



General
Mandatory

Passcode
Not configured

Restrictions
Not configured

Global HTTP Proxy
Not configured

Content Filter
Not configured

Domains
Not configured

Wi-Fi
Not configured

VPN
Not configured

AirPlay
Not configured

AirPrint

General


Name
Display name of the profile (shown on the device)
Secure Browser Profile

Organization
Name of the organization for the profile
[optional]

Description
Brief explanation of the contents or purpose of the profile
[optional]

Consent Message
A message that will be displayed during profile installation
[optional]

Cancel Save

- In the **General** section, in the *Name* field, enter a name for the profile.
- In the **Restrictions** section, click **Configure**. A list of restrictions appears.
- Make any required changes to the restrictions, or retain the default settings. Click **Save**. You return to the Settings tab, and the profile appears in the Profiles list.
- Click  to export the profile to the Mac.

Creation of the supervisory profile is complete.

Step 3: Place iPads in Autonomous Single App Mode

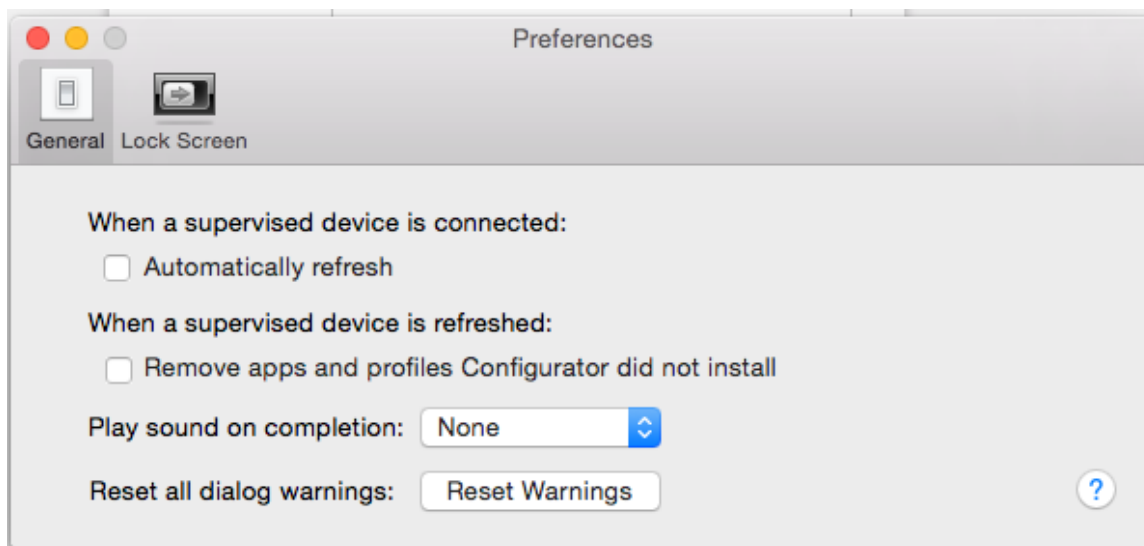


TIP: Installing on multiple iPads at once

Before starting this procedure, connect the iPads to the Mac through a USB hub. That way you can perform the installation on many of them at one time.

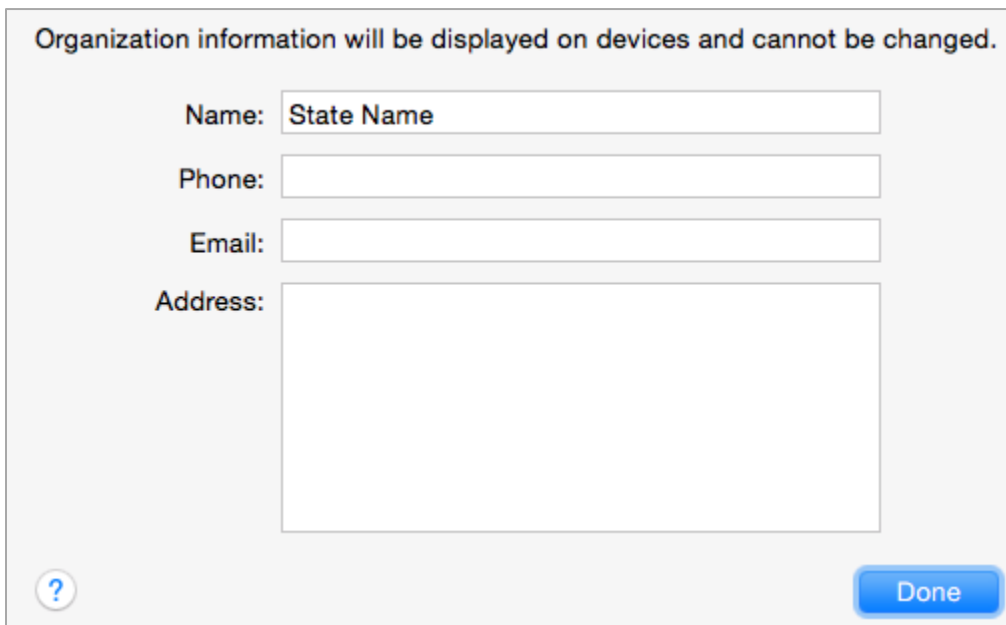
To install the MDM profile, supervisory profile, and secure browser:

1. On the Mac where you performed [Step 2: Create a Supervisory Profile](#), open the Apple Configurator.
2. From the **Apple Configurator** menu, select **Preferences**. The **Preferences** window opens.



3. Under **General**, clear the **Automatically refresh** and **Remove apps and profiles Configurator did not install** checkboxes.
4. Close the **Preferences** window.
5. Back in Apple Configurator, click **Prepare**, then **Settings**. The Settings window appears (see [Figure 1](#)).
6. In the *Name* field, enter a name to apply to the iPads.
7. *Optional:* Mark the **Number sequentially starting at 1** checkbox. This adds a number to each iPad's name. For example, if the *Name* field is Garden Elementary School1, and if three iPads are connected, each device receives the name Garden Elementary School 1, Garden Elementary School 2, and Garden Elementary School 3.
8. Set *Supervision* to **On**.

9. Click **Organization Info...** The **Organization Info** window appears.



Organization information will be displayed on devices and cannot be changed.

Name:

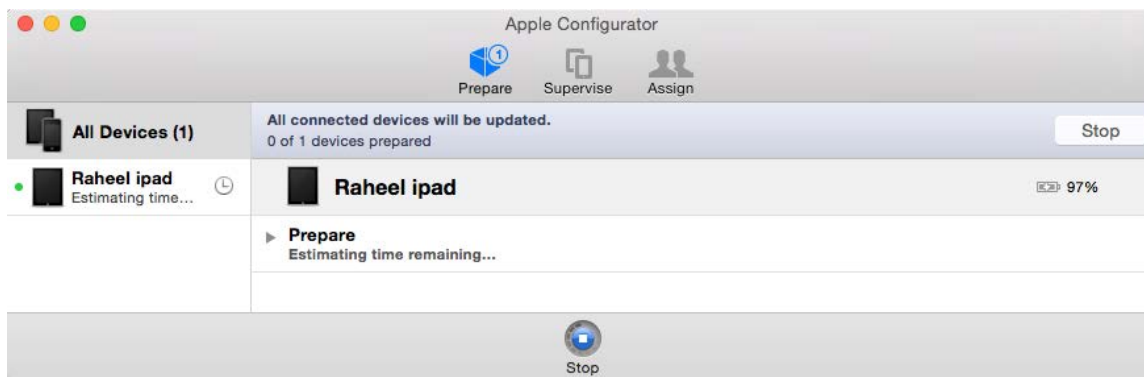
Phone:

Email:

Address:

10. In the *Name* field, enter MEA and then click **Done**. The **Organization Info** window closes.
11. If the profile you created in [Step 2: Create a Supervisory Profile](#) does not appear in the Profiles list, import it by doing the following:
- Click **+** below the Profiles list and select **Import Profile...**
 - Navigate to the profile you saved in step [7](#) on page [30](#), and after exporting the file, click **Open**.
12. Mark the checkbox for the profile you want to add to the iPads (see [Figure 1](#)).
13. Connect each iPad to the Mac via a USB cable or USB hub.
14. On each connected iPad, uninstall any existing versions of the secure browser.
15. In the Apple Configurator, under the Prepare tab, click **Prepare** at the bottom of the window. A confirmation message appears.

16. Click **Apply** in the confirmation message. Preparation starts and may take several minutes, after which the iPad restarts. The Apple Configurator displays progress messages during the preparation.



Note: iOS Upgrade

Apple Configurator may force the iPads to upgrade to the latest version of iOS.

17. After the iPad restarts, follow the prompts on the iPad to configure it until the home screen appears.
18. *Optional:* Confirm the supervisory profile is installed on the iPad. Go to **Settings > General > Profiles**. The profile name you used in step 4 on page 30 appears under Configuration Profiles.
19. On the iPad, download and install the MDM profile you created in [Step 1: Create a Mobile Device Management Profile](#).
20. After the MDM profile installation completes, install the secure browser onto the iPad. You can take a copy of the secure browser for iOS from <https://me.portal.airast.org>. (Detailed instructions for installing the secure browser are in the section “Installing the Secure Browser on iOS” of the *Secure Browser Installation Manual*.)
21. *Optional:* After installation completes, test it by doing the following:
 - a. Open the Secure Browser.
 - b. Log in to a test site.
 - c. Select a test, have the TA approve the test.
 - d. Start the test. The iPad enters ASAM.

22. Repeat steps [13–21](#) to prepare additional iPads.

23. In the Apple Configurator, click **Stop** and close the Apple Configurator.

Setting the iPad into ASAM is complete. When a student starts a test, the iPad enters ASAM mode. If needed, the bundle id is org.air.securebrowser.

Enabling the Secure Browser Keyboard on Android

The mobile secure browser for Android tablets requires the secure browser keyboard to be selected before students can access the login page. The reason for this is that the default Android keyboard allows predictive text, which would unduly aid students when entering written responses to test items. The secure browser keyboard is a basic keyboard, with no row for predictive text functionality.

The first time you open the Mobile Secure Browser on an Android tablet, you will be prompted to select the secure browser keyboard.



About the Secure Browser Keyboard and General Settings

Once the secure browser keyboard is set, it becomes the default keyboard for all Android tablet applications, not just the secure browser. If you want to return to the default Android keyboard after using the secure browser, you will need to navigate to Settings > Language & Input and uncheck the secure browser keyboard.

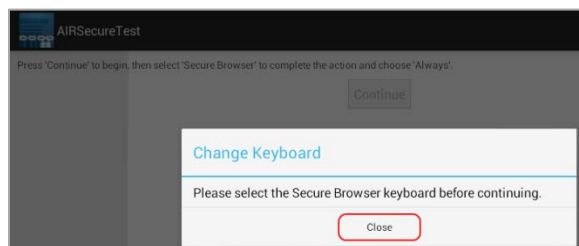
If you change back to the default Android keyboard, you will be prompted to select the secure browser keyboard the next time you open the secure browser. The secure browser will not allow you to access the student login page until the secure browser keyboard has been selected.

The following procedure describes how to enable the secure browser keyboard. The screen shots were taken with a Samsung Galaxy Tab 2; other Android versions may vary.

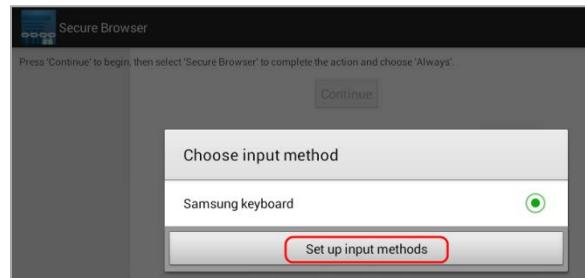
1. Select the secure browser icon on the home screen.



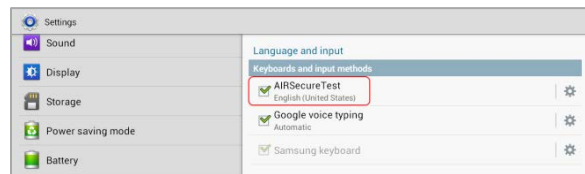
2. You will be prompted to change the keyboard. Select **Close**.



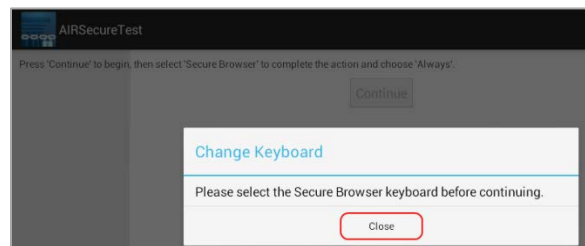
3. Select **Set up input methods**. The Language and Input settings screen will automatically open.



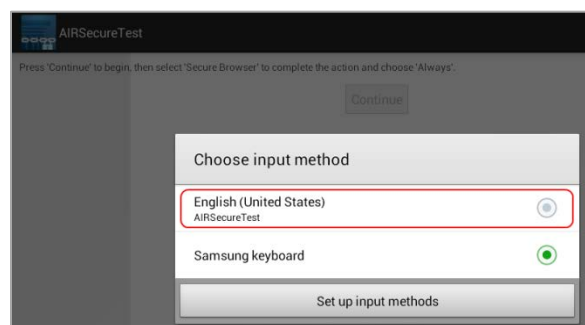
4. Select the checkbox next to "AIRSecureTest" so that a checkmark appears.
5. You will be prompted to acknowledge that this selection is okay. Select **OK** to continue. Note: This action allows the mobile secure browser to use the secure browser keyboard.



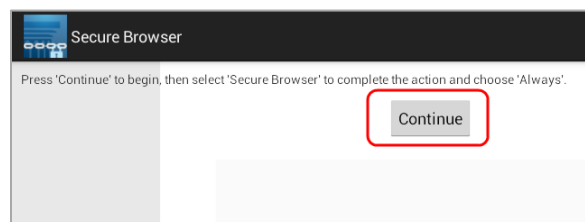
6. Navigate to the secure browser to open it. (You can use the application switcher or go back to "Home" and select the secure browser icon.)
7. You will be prompted to change the keyboard. Select **Close**.



8. The Android tablet's default keyboard will still be selected.
9. Select the checkmark or circle for the **AIRSecureTest** keyboard.



10. Select **Continue**. You will be prompted to complete the application launch using the preferred method.

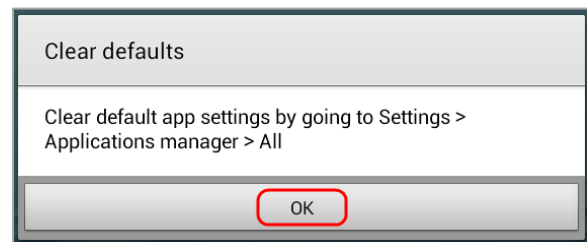


11. Select AIRSecureTest (ensure it is shaded and highlighted blue) and then select **Always**.

12. You will need to acknowledge that the secure browser's default settings have changed. (This is a result of selecting the secure browser keyboard.)



13. Select **OK**.



Enabling Kiosk Mode and Wiping Chrome OS

A secure browser application for Chromebooks is available from the Chrome Web Store. Using the AIRSecureTest kiosk application requires Chromebooks to run in kiosk mode. Instructions for installing the application and enabling kiosk mode are in the *Secure Browser Installation Manual*.

Non-managed Chromebooks must not already be configured with user accounts before you enable kiosk mode. If you have already added user accounts to Chromebooks, you will need to wipe the devices.

Google has provided instructions for wiping Chromebooks:
<https://support.google.com/chrome/a/answer/1360642?hl=en>.

After you wipe the Chromebooks, follow the instructions in the *Secure Browser Installation Manual* to enable kiosk mode and install the AIRSecureTest app.

Section IV. Text-to-Speech Requirements

This section contains information about text-to-speech requirements.

Overview of Text-to-Speech

Using text-to-speech requires at least one voice pack to be pre-installed on computers that will be used for testing. For Windows, Mac, Android, and Chrome operating systems, default voice packs are typically pre-installed. For computers running a Linux distribution, voice packs may need to be downloaded and installed. iPads have built-in voice packs.

A number of voice packs are available for desktop computers, and AIR researches and tests voice packs for compatibility with the secure browsers. Additionally, not all voice packs that come pre-installed with operating systems are approved for use with online testing. The voice packs listed at the end of this section have been tested and are whitelisted by the secure browser.

Using Text-to-Speech

Students using text-to-speech for the practice tests must log in using a supported secure browser. Students can also verify that text-to-speech works on their computers by logging in to a practice test session using their first name and student ID and selecting a test for which text-to-speech is available.



Note: We strongly encourage schools to test the text-to-speech settings before students take operational tests. You can check these settings through the diagnostic page. From the student test login screen, click the **Run Diagnostics** link, and then click the **Text-to-Speech Check** button.

How the Secure Browsers Work With Voice Packs

Desktop Secure Browsers

The secure browsers are configured to recognize several known voice packs to provide the text-to-speech accommodation. The secure browsers detect pre-installed voice packs on the students' machines. When a student who is using text-to-speech logs in to a test session and has been approved for testing, the secure browser will look for voice packs on the student's machine. When it recognizes an approved voice pack, the one with the highest priority rating will be used.

If any of the approved voice packs has also been set as the default voice on the computer, then that voice pack will always get the highest priority.

Mobile Secure Browsers

The mobile secure browser uses either the device's native voice pack or a voice pack embedded in the secure browser. If additional voice packs are downloaded to a tablet or Chromebook, they will not be recognized by the mobile secure browser.

iOS

Mobile Secure Browser version 2.2

- iOS 6.0–6.1: The embedded NeoSpeech voice pack will be used.
- iOS 7.0–7.1: The native iOS voice pack will be used.

Android

The AIRSecureTest app for Android uses the native voice pack available on the supported Android tablet being used.

Chrome OS

The AIRSecureTest kiosk app for Chromebooks uses the native voice pack available on the Chromebook device being used.

About NeoSpeech™ Voice Packs for Windows

Pursuant to an agreement between NeoSpeech™ and the American Institutes for Research (AIR), authorized users may download and install specific licensed NeoSpeech™ voice packs for use on supported Windows computers (Windows XP Service Pack 3, Vista, 7, 8.0, and 8.1).

These voice packs can be used instead of the default Windows voice packs for English. (The default Windows voice packs may still be used for text-to-speech, if desired.)

- The Julie voice pack is for English text-to-speech users.

The NeoSpeech™ voice pack is to be used only in conjunction with, and not separate from, the online assessments provided by AIR's Test Delivery System.

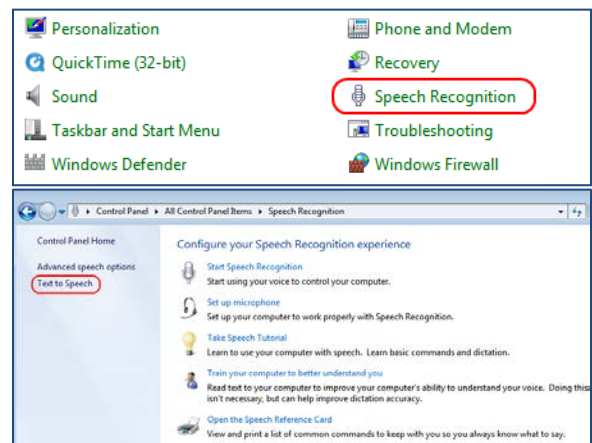
The NeoSpeech™ voice packs can be downloaded from TIDE. Installation instructions are also available in TIDE.

Windows Text-to-Speech Settings

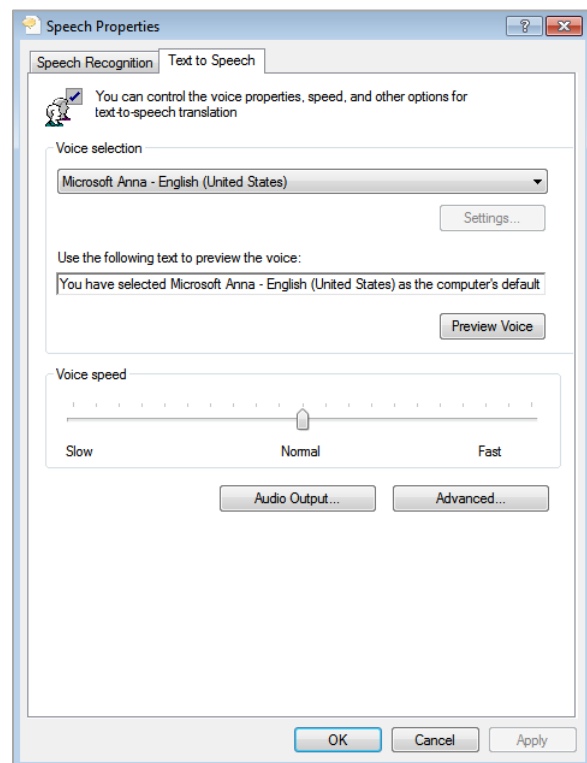
This section explains how to configure Windows for using text-to-speech with the secure browser. The text-to-speech feature is available on Windows versions as listed in the *System Requirements* document.

The instructions in this section are for Windows 7. The process is similar for other versions of Windows.

1. Open the Control Panel window, and select **Speech Recognition**.
2. In the Speech Recognition window, select **Text to Speech**.



3. Configure default text-to-speech preferences.
 - a. *Voice selection*: If multiple voice packs are available, select the default voice.
 - b. Select **Preview Voice** to see whether the selected voice requires a rate adjustment.
 - c. *Voice speed*: If necessary, adjust the voice speed. Drag the slider to make the voice speak slower or faster. To listen to the rate, select **Audio Output**.
 - d. When you are done, click **OK** to save your settings and then close the Speech Properties window.

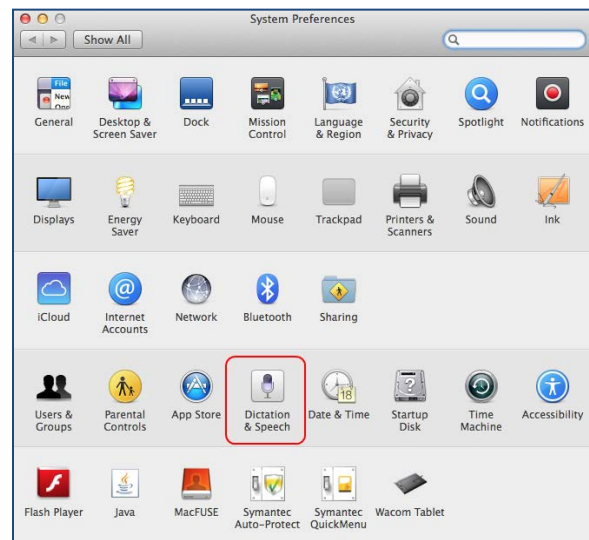


Mac OS X Text-to-Speech Settings

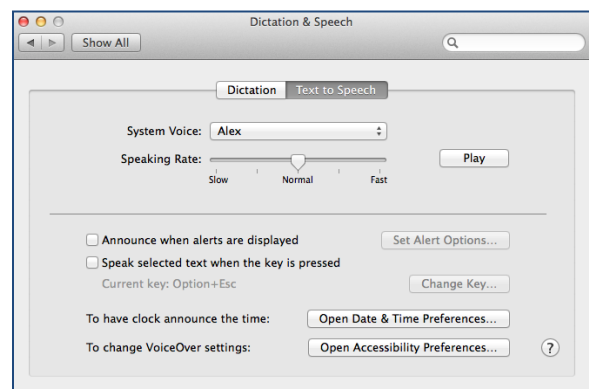
This section explains how to configure Mac OS X for using text-to-speech with the secure browser. The text-to-speech feature is available on OS X versions as listed in the *System Requirements* document.

The instructions in this section are for OS X 10.9. The process is similar for other versions of OS X.

1. Open System Preferences, and select **Dictation & Speech**.



2. In the Text to Speech section, configure your default text-to-speech preferences.
 - *System Voice*: If multiple voice packs are available, select the default voice.
 - Select **Play** to see whether the selected voice requires a rate adjustment.
 - *Speaking Rate*: If necessary, adjust the voice speed. Drag the slider to make the voice speak slower or faster. To listen to the rate, select **Play**.
 - When you are done, click the red **X** in the upper left corner to save your settings and close the Speech window.



Linux Text-to-Speech Settings

This section explains how to install voice packs on the supported Linux distributions.

1. Install Festival for text-to-speech:
 - Ubuntu: `sudo apt-get install festival`
 - Fedora, RedHat: `yum install festival`
 - openSUSE: `zypper install festival`
2. Install SoX for text-to-speech:
 - Ubuntu: `sudo apt-get install sox`
 - Fedora, RedHat: `yum install sox`
 - openSUSE: `zypper install festival`
3. Using [Table 6](#) as a reference, install voice packs.

Table 6. Commands for Installing Voice Packs on Linux Distributions

Voice	Command
Ubuntu	
American English male	<code>sudo apt-get install festvox-kallpc16k</code>
openSUSE	
Kevin American male	<code>zypper install festvox-kal-diphone</code>
Kurt American male	<code>zypper install festvox-ked-diphone</code>
Fedora, RedHat	
Kevin American male	<code>yum install festvox-kal-diphone</code>
Kurt American male	<code>yum install festvox-ked-diphone</code>

Voice Packs Recognized by Desktop Secure Browsers

Tables 7–9 display the voice packs for each desktop operating system (Windows, Mac, and Linux) that are currently recognized by the secure browser.

Windows and Mac OS X computers typically ship with at least one default voice pack. Many of these default voice packs are recognized by the secure browser.

Windows

Table 7. Voice Packs Recognized by Secure Browsers—Windows

Vendor	Voice Pack	Language
Windows (pre-installed)	Julie	English
Windows (pre-installed)	Kate	English
Windows (pre-installed)	Michael	English
Windows (pre-installed)	Michelle	English
Windows (pre-installed)	MSAnna	English
Windows (pre-installed)	MS_EN-GB_HAZEL	English
Windows (pre-installed)	MS_EN-US_DAVID	English
Windows (pre-installed)	MS_EN-US_ZIRA	English
Windows (pre-installed)	MSMary	English
Windows (pre-installed)	MSMike	English
Windows (pre-installed)	MSSam	English
Windows (pre-installed)	Paul	English
Windows (pre-installed)	Violeta	Spanish
Cepstral (commercial)	Cepstral_David	English
Cepstral (commercial)	Cepstral_Marta	Spanish
Cepstral (commercial)	Cepstral_Miguel	Spanish
NeoSpeech (commercial)	VW Julie	English
NeoSpeech (commercial)	VW Violeta	Spanish

Mac OS X

Table 8. Voice Packs Recognized by Secure Browsers—Mac OS X

Vendor	Voice Pack	Language
Mac (pre-installed)	Agnes	English
Mac (pre-installed)	Alex	English
Mac (pre-installed)	Bruce	English
Mac (pre-installed)	Callie	English
Mac (pre-installed)	David	English
Mac (pre-installed)	Fred	English
Mac (pre-installed)	Jill	English
Mac (pre-installed)	Junior	English
Mac (pre-installed)	Kathy	English
Mac (pre-installed)	Princess	English
Mac (pre-installed)	Ralph	English
Mac (pre-installed)	Samantha	English
Mac (pre-installed)	Tom	Spanish
Mac (pre-installed)	Vicki	English
Mac (pre-installed)	Victoria	English
Mac (pre-installed)	Diego	Spanish
Mac (pre-installed)	Javier	Spanish
Mac (pre-installed)	Marta	Spanish
Mac (pre-installed)	Monica	Spanish
Mac (pre-installed)	Paulina	Spanish
Infovox (commercial)	Heather Infovox iVox HQ	English
Infovox (commercial)	Rosa Infovox iVox HQ	Spanish

Linux

Table 9. Voice Packs Recognized by Secure Browsers—Linux

Vendor	Voice Pack	Language
Festvox (commercial)	cmu_us_awb_arctic_hts	English
Festvox (commercial)	cmu_us_bdl_arctic_hts	English
Festvox (commercial)	cmu_us_jmk_arctic_hts	English
Festvox (commercial)	cmu_us_slt_arctic_hts	English
Festvox (commercial)	kal_diphone	English
Festvox (commercial)	ked_diphone	English

Appendix A. Systems and URLs Provided by AIR

This appendix provides information about the URLs for each system that AIR provides.

Non-Testing Sites

System	URL
Portal and secure browser installation files	http://me.portal.airast.org/browsers/
Single Sign On System	https://me.sso.airast.org/auth/UI/Login
Test Information Distribution Engine	me.tide.airast.org
Online Reporting System	me.reports.airast.org

Testing Sites

TA and Student Testing Sites

The Test Administrator and student testing sites use a cloud-based satellite system for optimal load balancing during testing. Testing servers and satellites may be added or modified during the school year to ensure an optimal testing experience. As a result, AIR strongly encourages you to whitelist at the root level. This requires using a wildcard.

System	URL
TA and Student Testing Sites	*.tds.airast.org

Online Dictionary and Thesaurus

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The Merriam-Webster URLs listed below should also be open or whitelisted to ensure that students can use the dictionary and thesaurus tool.

URL	IP Address
http://media.merriam-webster.com	64.124.231.250
http://www.dictionaryapi.com	64.124.231.250

Appendix B. Technology Coordinator Checklist

This checklist can be printed out and referred to during review of networks and computers used for testing.

	Activity	Estimated Time to Complete	Target Completion Date	Reference
<input type="checkbox"/>	Verify that all of your school's computers that will be used for online testing meet the operating system requirements.	5–10 hours	3–4 weeks before testing begins in your school	<i>System Requirements</i>
<input type="checkbox"/>	Verify that your school's network and Internet are properly configured for testing, conduct network diagnostics, and resolve any issues.	5–10 hours	3–4 weeks before testing begins in your school	Network and Internet Requirements
<input type="checkbox"/>	Install the secure browser on all computers that will be used for testing.	5–10 hours	3–4 weeks before testing begins in your school	<i>Secure Browser Installation Manual</i>
<input type="checkbox"/>	Enable pop-up windows and review software requirements for each operating system.	5–10 hours	1–2 weeks before testing begins in your school	General Software Requirements
<input type="checkbox"/>	On Windows computers, disable Fast User Switching. If a student can access multiple user accounts on a single computer, you are encouraged to disable the Fast User Switching function.	5–10 hours	1–2 weeks before testing begins in your school	Disabling Fast User Switching
<input type="checkbox"/>	On Mac 10.7, 10.8, 10.9, and 10.10 computers, disable Spaces in Mission Control.	5–10 hours	1–2 weeks before testing begins in your school	Disabling Spaces
<input type="checkbox"/>	Install and verify any required text-to-speech software onto computers that will be used for testing.	5–10 hours	1–2 weeks before testing begins in your school	Text-to-Speech Requirements
<input type="checkbox"/>	On iPads , ensure that Guided Access or ASAM is enabled and that TAs know how to activate Guided Access.	5–10 hours	1–2 weeks before testing begins in your school	Enabling Guided Access on iOS

	Activity	Estimated Time to Complete	Target Completion Date	Reference
<input type="checkbox"/>	On Android tablets, ensure that the secure browser keyboard is enabled.	5–10 hours	1–2 weeks before testing begins in your school	Enabling the Secure Browser Keyboard on Android

Appendix C. User Support

If this document does not answer your questions, please contact the Maine Help Desk.

The Help Desk will be open Monday–Friday from 7:00 a.m. to 7:00 p.m. Eastern Time during the summative testing window and from 8:00 a.m. to 5:00 p.m. Eastern Time outside of the summative testing window (except holidays).

Maine Help Desk

Toll-Free Phone Support: 1-844-560-7814

Email Support: mehelpdesk@air.org

If you contact the Help Desk, you will be asked to provide as much detail as possible about the issues you encountered.

Include the following information:

- Test Administrator name and IT/network contact person and contact information
- SSIDs of affected students
- Results ID for the affected student tests
- Operating system and browser version information
- Any error messages and codes that appeared, if applicable
- Information about your network configuration:
 - Secure browser installation (to individual machines or network)
 - Wired or wireless Internet network setup